



# **Qualified certification authority**

## **User statement (qualified certificates) version 1.1**

Document type:

**Operational document**

Document identification:

**QCA D40**

**January 2009**

Version	Date	Approved by	Notes
0.1	26/JUL/2005	Manager QCA	first version
1.01	05/SEP/2005	Manager QCA	minor changes in document
1.02	16/SEP/2006	Manager QCA	added information about issuing the subsequent certificates
1.1	12/JAN/2009	Manager QCA	document structure has changed; added list of performed audits; added information about claim process

# Content

<b>1 Introduction.....</b>	<b>4</b>
1.1 Scope of document.....	4
1.2 List of performed audits and inspections.....	4
<b>2 Contact information.....</b>	<b>4</b>
2.1 Provider of certification services.....	4
2.2 Contact offices to provide certification services.....	4
2.3 Communication with clients.....	5
2.4 Information publication.....	5
<b>3 Certificate types and verification procedures.....</b>	<b>5</b>
3.1 Types of issued certificates.....	5
3.2 Applicant verification when issuing first certificate.....	6
3.3 Applicant verification when issuing subsequent certificate.....	6
<b>4 Limited use.....</b>	<b>6</b>
<b>5 Obligations of clients ant their representatives.....</b>	<b>6</b>
<b>6 Basic obligations of the depending parties and other users.....</b>	<b>7</b>
<b>7 Guarantee and responsibility limitation.....</b>	<b>7</b>
<b>8 Contracts and certification policies.....</b>	<b>8</b>
<b>9 Protection of personal data.....</b>	<b>8</b>
<b>10 Compensation policy and claim process.....</b>	<b>8</b>
<b>11 Legal environment.....</b>	<b>9</b>
<b>12 Accreditation and verification of security compliance.....</b>	<b>9</b>

# 1 Introduction

## 1.1 Scope of document

This document gives the basic overview of the hierarchy of the certification authorities PostSignum QCA, rights and duties of the holders of certificates issued by PostSignum Qualified CA and depending parties.

This document is just informative, it does not replace the certification policies and does not form a part of the Contract on the provision of the certification services between the client and the Czech Post, national enterprise (further referred to as Czech Post or CP).

## 1.2 List of performed audits and inspections

Date	Type of audit/inspection	Verdict of control authority
December 21, 2008	Keeping audit on certification against ISO 9001 and ISO 27001, made by CQS company.	Is consistent
March 27, 2008	Verification of security compliance, made by Deloitte company.	Meets the criteria
December 19, 2007	Audit on certification against ISO 9001 and ISO 27001, made by CQS company.	Is consistent
December 30, 2006	Verification of security compliance, made by Ernst & Young company.	Meets the criteria
June 23, 2005	Verification of security compliance to get the accreditation, made by Ernst & Young company.	Meets the criteria

# 2 Contact information

## 2.1 Provider of certification services

Provider of PostSignum QCA certification services is:  
Czech Post, national enterprise, ID No. 47114983  
Politických vězňů street 909/4  
225 99 Prague 1  
Czech Republic

## 2.2 Contact offices to provide certification services

Business and contact places of PostSignum QCA make the contracts with customers. Contact information can be found on the PostSignum QCA web server.

Contact places provide the service of certificate issuing.

The following office provides nonstop certificate revocation:  
Czech Post, national enterprise

Office of user support QCA/VCA  
Wolkerova street 480  
749 20 Vítkov  
Czech Republic  
email: [postsignum@cpost.cz](mailto:postsignum@cpost.cz)  
fax: +420 556 316 292  
phone: +420 556 316 290

## **2.3 Communication with clients**

Contact offices providing certification services can handle questions about the certification services.

The following will answer special questions:

Czech Post, national enterprise  
Office of development QCA/VCA  
Sazečská street 603/9  
225 99 Prague 10  
Czech Republic  
email: [admca.vakph@cpost.cz](mailto:admca.vakph@cpost.cz)

The questioner obtains the answer within three working days.

## **2.4 Information publication**

This user statement, certification policies and other public information can be found on PostSignum QCA web server:  
<http://qca.postsignum.cz>

# **3 Certificate types and verification procedures**

## **3.1 Types of issued certificates**

The Czech Post has established a two-level hierarchy of certification authorities with the name of PostSignum QCA. The root of this hierarchy is the certification authority PostSignum Root QCA, which issued the certificate for the certification authority PostSignum Qualified CA.

PostSignum Qualified CA issues certificates to end users. Two basic models of registration in relation to the end user are applied. The first model of registration aims at the legal entities and entrepreneurial natural persons, the second at individuals – nonentrepreneurial natural persons.

PostSignum Qualified CA issues these types of certificates:

- qualified certificates for the verification of the electronic signature of the employee,
- qualified system certificates of the organization for the verification of the electronic mark,
- qualified certificates for the verification of the electronic signature of the natural person,

- qualified system certificates for the verification of the electronic mark of the natural person.

Certificates of the public keys issued within the hierarchy of PostSignum QCA comply with the X.509 v3 standard.

### **3.2 Applicant verification when issuing first certificate**

During the process of the certificate issuing the identity of the applicant is always verified through his/her personal documents and, in case of the certificate for the legal entity or entrepreneurial natural person also the relation of the applicant for the certificate to this person.

Applicant must be physically present at the process of certificate issuing. He/she cannot delegate his/her plenipotentiary.

Detailed description of the registration methods is stated in the corresponding certification policies.

### **3.3 Applicant verification when issuing subsequent certificate**

During the process of the subsequent certificate issuing the identity of the applicant is verified through the verification of the electronic signature on the request for subsequent certificate.

Detailed description of the registration methods is stated in the corresponding certification policies.

## **4 Limited use**

Qualified certificates and qualified system certificates issued by PostSignum QCA may be used only for the verification of the electronic signature or the electronic mark (according to the type of the certificate) in accordance with the valid legal regulations.

Qualified certificates and qualified system certificates issued by PostSignum QCA are not designed for the communication or transactions in the areas with the high risk of damages to property or health, i.e. chemical plants, air traffic, nuclear plants, etc., or in areas related to the security and defensibility of the state.

## **5 Obligations of clients and their representatives**

The client of PostSignum QCA is a legal entity or natural person, who enters into the corresponding contractual relations with the Czech Post. The client is especially required to

- give correct and full information when making a contract on the provision of certification services,
- immediately notify the provider of the certification services of the changes of the data stated in the contract or certificate.

The applicant for the certificate is a natural person who asks, on behalf of the client, for the issuing of the certificate and administers the issued certificate (in case of the client-

nonentrepreneurial natural person the applicant for the certificate is the client.). The applicant is especially required to

- become familiar with the certification policy under which the certificate is to be issued,
- give the provider of the certification services correct and full information,
- immediately notify the provider of the certification services of the changes in the data stated in the contract on the provision of the certification services or in the issued certificate,
- deal with the private key, which corresponds to the public key in the certificate issued under any certification policy, with a due care so that no illegal misuse is possible, and use the private key only for the purposes stated in the certification policy under which the corresponding certificate has been issued,
- notify the provider of the certification services without delay of the facts leading to the revocation of the certificate, especially of the suspicion that the private key has been misused, and ask for the revocation of the certificate.

## **6 Basic obligations of the depending parties and other users**

Depending parties and other users must especially

- obtain certificates of the PostSignum Qualified CA and PostSignum Root QCA certification authorities from a safe source and verify the fingerprint of these certificates,
- prior to using a certificate issued by PostSignum Qualified CA verify the validity of the PostSignum Qualified CA and PostSignum Root QCA certificates and then also the validity of the issued end certificate,
- consider sufficiently (especially on the basis of the knowledge of the corresponding certification policy), whether the certificate issued by PostSignum Qualified CA under the corresponding policy is appropriate for the purpose he/she wants to use it for.

## **7 Guarantee and responsibility limitation**

The Czech Post undertakes to fulfill all duties imposed under the certification policies under which the certificates are issued and mandatory provisions of the corresponding legal regulations.

The Czech Post gives the above mentioned guarantees for the whole period of the validity of the contract on the provision of the certification services made with the client.

Guarantees listed above are exclusive guaranties of the Czech Post and the Czech post does not provide any other guaranties.

The Czech Post is not responsible for the defects in the services provided which arose from the reasons of incorrect or illegal use of the services provided within the framework of the performance of the contract on the provision of the certification services by the holder, especially for the operation in contradiction with the conditions stated in the certification policy, as well as defects resulting from the act of god, including the temporary interruption of the telecommunication links, etc. The Czech Post cannot be held responsible for the damage resulting from the use of the qualified certificate or qualified system certificate after

the request for its revocation has been submitted, on condition that the Czech Post observes the time limits for the publication of the revoked qualified certificate or the qualified system certificate on the certificate revocation list (CRL).

## **8 Contracts and certification policies**

The relationship between the client and the Czech Post as a provider of the certification services is (apart from the corresponding provisions of the mandatory legal regulations) specified by the contract whose parts are, among others

- General business conditions of the electronic services of CP,
- valid certification policies, and
- current price list.

The relationship between the depending parties and the Czech Post (as a provider of the certification services) is defined by the corresponding provisions of the valid certification policies.

The relationship between the Czech Post and depending parties is not regulated by a contract.

All the above mentioned documents are available on the PostSignum QCA web server, or at the contact places of PostSignum QCA.

## **9 Protection of personal data**

The Czech Post ensures the protection of the personal data of the persons delivered to the Czech Post during the provision of certification services. Principles of the protection of the personal data are included in the certification policies, general business conditions, and in the current Certification Practice Statement, and results from the corresponding provisions of the law No. 101/2000 Coll. on the protection of the personal data in the wording of later regulations.

The applicant for the certificate gives his/her consent to the Czech Post to process the personal data necessary for the issuing and revocation of the certificate with the required data.  
text

## **10 Compensation policy and claim process**

In case of non-delivery of the services in the required quality (for example issuing of the certificate with the wrong content), the client is entitled to the return of the whole price for the corresponding service or the provision of the new service free of charge.

The PostSignum QCA client delivers the claim request to contact places of PostSignum QCA or to the Helpdesk office. PostSignum QCA claim office reviews the request validity within three working days. The client is notified about the decision by e-mail or mail. A form of compensation is arranged with client, if applicable.

## **11 Legal environment**

The activities of PostSignum QCA follow the corresponding provisions of the legal code of the Czech Republic, especially

- law No. 227/2000 Coll. on the electronic signature in wording of later regulations,
- regulation No. 366/2001 from July 16, 2006, on the processes of qualified providers of certification services,
- law No. 101/2000 Coll. on the protection of personal data in wording of later regulations.

## **12 Accreditation and verification of security compliance**

The Czech Post as a provider of the PostSignum QCA certification services became on August 3, 2005, an accredited provider of the certification services based on the accreditation awarded by the Ministry of Information of the Czech Republic.

PostSignum QCA information system was certified against the ISO 9001:2001 (Quality Management System) and ISO 27001 (Information Security Management System) on December 21, 2007.

The activity of PostSignum QCA is subjected to audit and inspections, which are made by Czech Post employees or by external auditor independent on the Czech Post, national enterprise. The intervals of the audits are specified in the certification policies.